信息安全漏洞周报

（2023 年第 41 期 总第 698 期）

信息安全测评中心 **2023 年 10 月 15 日**

根据国家信息安全漏洞库（CNNVD）统计，本周（2023 年 10 月 9 日至 2023 年 10 月 15 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 647 个。

接报漏洞情况

本周 CNNVD 接报漏洞 13852 个，其中信息技术产品漏洞（通用型漏洞）178 个，网络信息系统漏洞（事件型漏洞）16 个，漏洞平台推送漏洞 13658 个。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞647个，漏洞新增数量有所上升。从厂商分布来看微软公司新增漏洞最多，有104个；从漏洞类型来看，跨站请求伪造类的安全漏洞占比最大，达到10.20%。新增漏洞中，超危漏洞57个，高危漏洞279个，中危漏洞302个，低危漏洞9个。

（一） 安全漏洞增长数量情况

本周CNNVD采集安全漏洞647个。

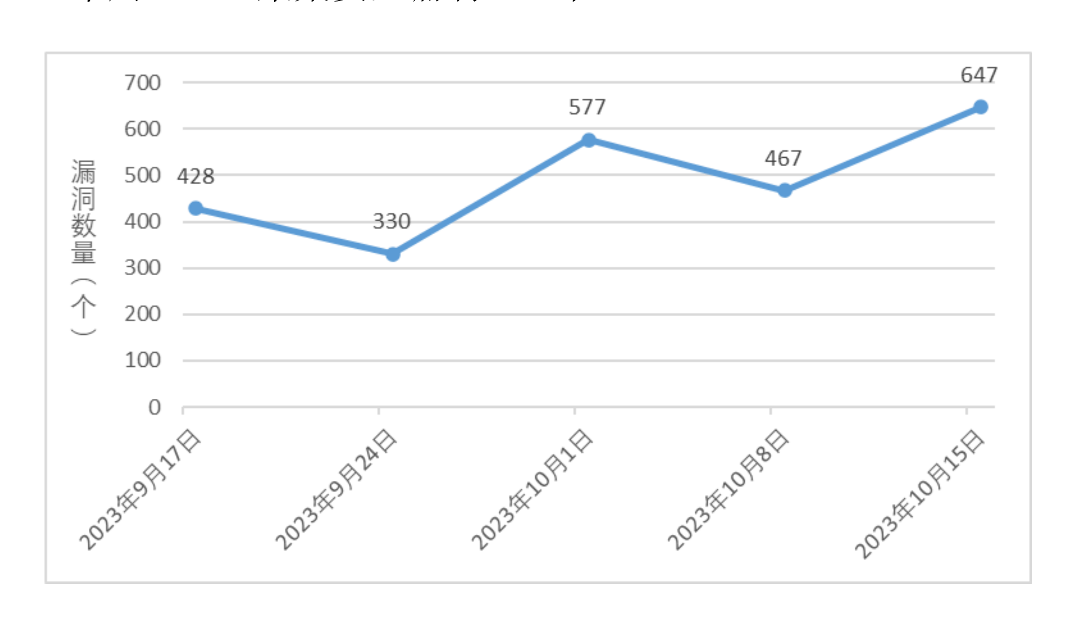


图1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，微软公司新增漏洞最多，有104个。各厂商漏洞数量分布如表1所示。

表1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	微软	104	16.07%
2	WordPress基金会	70	10.82%

3	Fortinet	37	5.72%
4	谷歌	30	4.64%
5	Juniper Networks	30	4.64%

本周国内厂商漏洞 54 个，华为公司漏洞数量最多，有 22 个。国内厂商漏洞整体修复率为 66.67%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，跨站请求伪造类的安全漏洞占比最大，达到 10.20%。漏洞类型统计如表 2 所示。

表 2 漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	跨站请求伪造	66	10.20%
2	缓冲区错误	36	5.56%
3	跨站脚本	34	5.26%
4	代码问题	30	4.64%
5	操作系统命令注入	23	3.55%
6	SQL 注入	15	2.32%
7	资源管理错误	12	1.85%
8	竞争条件问题	12	1.85%
9	信息泄露	10	1.55%
10	输入验证错误	7	1.08%
11	命令注入	6	0.93%
12	授权问题	4	0.62%
13	路径遍历	4	0.62%
14	访问控制错误	4	0.62%
15	日志信息泄露	4	0.62%

16	信任管理问题	3	0.46%
17	数据伪造问题	3	0.46%
18	代码注入	2	0.31%
19	数字错误	1	0.15%
20	环境问题	1	0.15%
21	其他	370	57.19%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 57 个，高危漏洞 279 个，中危漏洞 302 个，低危漏洞 9 个。相应修复率分别为 66.67%、90.32%、80.79%和 77.78%。根据补丁信息统计，合计 541 个漏洞已有修复补丁发布，整体修复率为 83.62%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	57	38	66.67%
2	高危	279	252	90.32%
3	中危	302	244	80.79%
4	低危	9	7	77.78%
合计		647	541	83.62%

（四） 本周重要漏洞实例

本周重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	缓冲区错误	CNNVD-202310-903	谷歌	Google Pixel 缓冲区错误漏洞	是	超危

2	SQL 注入	CNNVD-202310-946	WordPress 基金会	WordPress plugin MainWP Google Analytics Extension SQL 注入漏洞	是	高危
3	其他	CNNVD-202310-742	微软	Microsoft ODBC Driver 安全漏洞	是	高危

1. Google Pixel 缓冲区错误漏洞（CNNVD-202310-903）

Google Pixel 是美国谷歌（Google）公司的一款智能手机。

Google Pixel 存在安全漏洞，该漏洞源于 TBD 组件缺少边界检查，从而导致堆栈缓冲区溢出。攻击者利用该漏洞可以远程执行代码。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://source.android.com/security/bulletin/pixel/2023-10-01

2. WordPress plugin MainWP Google Analytics Extension SQL 注入漏洞（CNNVD-202310-946）

WordPress 和 WordPress plugin 都是 WordPress 基金会的产品。WordPress 是一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。WordPress plugin 是一个应用插件。

WordPress plugin MainWP Google Analytics Extension 4.0.4 版本及之前版本存在 SQL 注入漏洞。攻击者利用该漏洞可执行 SQL 注入攻击。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://wpscan.com/plugin/mainwp-google-analytics-extension/

3. Microsoft ODBC Driver 安全漏洞（CNNVD-202310-742）

Microsoft ODBC Driver 是美国微软（Microsoft）公司的一种驱动程序。允许应用程序使用 SQL 作为访问数据的标准来访问数据库管理系统（DBMS）中的数据。

Microsoft ODBC Driver 存在安全漏洞。攻击者利用该漏洞可以远程执行代码。以下产品和版本受到影响：Microsoft SQL Server 2019 for x64-based Systems (GDR),Microsoft SQL Server 2022 for x64-based Systems (GDR),Microsoft ODBC Driver 17 for SQL Server on Windows,Microsoft ODBC Driver 17 for SQL Server on Linux,Microsoft ODBC Driver 17 for SQL Server on MacOS,Microsoft ODBC Driver 18 for SQL Server on Windows,Microsoft ODBC Driver 18 for SQL Server on Linux,Microsoft ODBC Driver 18 for SQL Server on MacOS,Microsoft SQL Server 2022 for x64-based Systems (CU 8),Microsoft SQL Server 2019 for x64-based Systems (CU 22)。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36730

二、漏洞平台推送情况

本周 CNNVD 接收漏洞平台推送漏洞 13658 个。

表 5 本周漏洞平台推送情况

序号	漏洞平台	漏洞总量
1	补天平台	11007
2	漏洞盒子	2348
3	360 漏洞云	303
推送总计		13658

三、接报漏洞情况

本周 CNNVD 接报漏洞 194 个，其中信息技术产品漏洞（通用型漏洞）178 个，网络信息系统漏洞（事件型漏洞）16 个。

表 6 本周漏洞报送情况

序号	报送单位	漏洞总量
1	北方实验室（沈阳）股份有限公司	12
2	个人	12
3	北京中睿天下信息技术有限公司	9
4	奇安信网神信息技术（北京）股份有限公司	9
5	浙江大华技术股份有限公司	8
6	北京启明星辰信息安全技术有限公司	7
7	北京五一嘉峪科技有限公司	7
8	杭州迪普科技股份有限公司	7
9	山东泽鹿安全技术有限公司	7
10	北京安天网络安全技术有限公司	6
11	河南灵创电子科技有限公司	6
12	远江盛邦(北京)网络安全科技股份有限公司	6
13	中控技术股份有限公司	6
14	烽台科技（北京）有限公司	5
15	广州竞远安全技术股份有限公司	5
16	北京墨云科技有限公司	4
17	联通数字科技有限公司	4
18	云南启安科技有限公司	4
19	中电信数智科技有限公司	4
20	北京微步在线科技有限公司	3

21	北京云起无垠科技有限公司	3
22	广州锦行网络科技有限公司	3
23	杭州安恒信息技术股份有限公司	3
24	杭州默安科技有限公司	3
25	河南悦海数安科技有限公司	3
26	软安科技有限公司	3
27	上海文鳐信息科技有限公司	3
28	网宿科技股份有限公司	3
29	长扬科技（北京）股份有限公司	3
30	北京华云安信息技术有限公司	2
31	北京灰度科技有限公司	2
32	北京时代新威信息技术有限公司	2
33	北京小佑网络科技有限公司	2
34	超聚变数字技术有限公司	2
35	杭州孝道科技有限公司	2
36	湖北肆安科技有限公司	2
37	南京国云电力有限公司	2
38	南京聚铭网络科技有限公司	2
39	深圳融安网络科技有限公司	2
40	亚信科技（成都）有限公司	2
41	北京安普诺信息技术有限公司	1
42	北京奇虎科技有限公司	1
43	北京摄星科技有限公司	1
44	北京威努特技术有限公司	1

45	成都星云智联科技有限公司	1
46	杭州海康威视数字技术股份有限公司	1
47	河南东方云盾信息技术有限公司	1
48	湖南罗洪科技有限公司	1
49	华为技术有限公司	1
50	任子行网络技术股份有限公司	1
51	赛尔网络有限公司	1
52	山西轩辕信息安全技术有限公司	1
53	上海齐同信息科技有限公司	1
54	中国电信股份有限公司网络安全产品运营中心	1
报送总计		194

四、收录漏洞通报情况

本周 CNNVD 收录漏洞通报 166 份。

表 7 本周漏洞通报情况

序号	报送单位	通报总量
1	南京禾盾信息科技有限公司	22
2	中国电信股份有限公司网络安全产品运营中心	12
3	北京神州绿盟科技有限公司	8
4	北京奇虎科技有限公司	7
5	奇安信网神信息技术（北京）股份有限公司	7
6	新华三技术有限公司	7
7	北京华云安信息技术有限公司	6
8	河南灵创电子科技有限公司	6
9	北京六方云信息技术有限公司	5

10	杭州迪普科技股份有限公司	5
11	联通数字科技有限公司	5
12	深信服科技股份有限公司	5
13	北京小佑网络科技有限公司	4
14	广州纬安科技有限公司	4
15	杭州安恒信息技术股份有限公司	4
16	湖南省金盾信息安全等级保护评估中心有限公司	4
17	华为技术有限公司	4
18	北京天融信网络安全技术有限公司	3
19	北京微步在线科技有限公司	3
20	北京云科安信科技有限公司	3
21	北京知道创宇信息技术股份有限公司	3
22	杭州海康威视数字技术股份有限公司	3
23	南京国云电力有限公司	3
24	锐捷网络股份有限公司	3
25	上海斗象信息科技有限公司	3
26	深圳市魔方安全科技有限公司	3
27	天翼数智科技（北京）有限公司	3
28	北京安胜华信科技有限公司	2
29	北京山石网科信息技术有限公司	2
30	贵州泰若数字科技有限公司	2
31	河南悦海数安科技有限公司	2
32	浪潮电子信息产业股份有限公司	2

33	内蒙古旌云科技有限公司	2
34	亚信科技（成都）有限公司	2
35	长扬科技（北京）股份有限公司	2
36	北京安博通科技股份有限公司	1
37	北京安天网络安全技术有限公司	1
38	北京赛博昆仑科技有限公司	1
39	北京威努特技术有限公司	1
40	北京智游网安科技有限公司	1
收录总计		166